MINESH PANDYA
PRINCIPAL
HKA

Trends shaping cyber resilience in the energy sector

As first published in online in Enlit World, 22 February 2022.

Introduction
The Electricity, Oil and Gas and Civil Nuclear sectors have recently seen improved cyber resilience as a result of regulations such as the European Union (EU) Networks & Information Systems (NIS) Directive, but there is still work to be done as rapid technology advancements within these sectors bring a plethora of cyber risks that, if left unaddressed, can severely harm these critical infrastructures and their customers.

The reason for the energy sector's present cyber challenges is examined in this article. We explore the drivers for advances in technology such as the Internet of Things (IoT), Microgrids, Virtual Power Plants (VPP), cloud services, and digitisation, as well as how the technology adoption by the sector has created more cyber risks.

Protecting against current threats and risks
Historically, investment within the energy sector for business-as-usual activities tended to follow the life span of equipment such as transformers or generators. Until recently, Information Technology (IT) systems were viewed as supporting technologies to ensure the reliability of this equipment. As a result, when compared to other sectors that tend to refresh IT systems more frequently, the investment cycle (and therefore lifespan) for these IT systems is relatively extended within the energy sector. The growing use of these IT systems is largely due to advances in technology and equipment, which means that these systems are now vital to guarantee the energy sector's desired level of reliability and resilience.

While it is essential to integrate IT systems to support new technologies and modernise the energy sector, these systems often share the same network as critical equipment which adds complexity, introduces new dependencies and exposes potential cyber vulnerabilities. These energy IT systems are subject to the same threats and risks as general-purpose IT systems used in other industries but investment cycles, previously limited connectivity, usage, performance demands and communication methods that negated the investment case for regular upgrades. As a result of these historical issues, combined with recent technological advancements, the energy sector faces a unique challenge in terms of cyber resilience.

Adoption and integration of new technologies
Due to lower adoption of new technologies to date and tighter regulation, this cyber issue is a higher concern in the electricity and oil and gas sub-sector, and less so for civil nuclear. IoT is helping develop new innovative services for customers, such as smart meters in the electricity sector, as well as improving efficiency and monitoring for equipment at remote locations in the upstream oil sub-sector. IoT devices increase the attack surface for a prospective attacker, posing key cyber challenges such as preventing physical attacks against the device itself, securing communication and ensuring security by design in crucial domains like software development and authentication.

The need for modernisation of the energy sector is largely driven by the growing use of renewable resources, and more complex power requirements that drive technologies like microgrids and virtual power plants. Other

emerging cyber challenges are securing 'big data' technologies as a result of increased analytics, as well as securing expanding telecommunications infrastructures and networks as a result of growing usage of mobile devices and new applications

Microgrids aid in the resilience of local power supplies and can leverage local renewable power generation by operating independently from the main grid as needed, such as to support critical services such as health or the military in the event of a natural disaster. As microgrids become more complex, they require computer networks to control and manage them, and as such become more vulnerable to cyber-attacks. The impact of such attacks could have consequences such as cost for business disruption and damage to equipment, as well as potential power losses in critical scenarios.

Virtual Power Plants (VPP) are another fast-growing distributed energy resource technology. They integrate several localised power generating units through interconnection and smart central control rooms to enhance generation, as well as trade it in the electricity market. Due to the nature of the architecture in a VPP, which typically comprises of many interconnected devices, attacks can potentially take place on any of the devices, rendering the entire network inaccessible if a successful cyber-attack were launched. As VPP's grow, as will the expense and impact of cost and disruption.

Cloud services and digitisation

Due to increasing cost pressure and the growing demand for data services and dedicated telecommunication networks, the introduction of these new services and technologies has led to a search for improved operational efficiency. As a result, the previously dependable energy sector is becoming reliant on other sectors, such as cloud service providers, which typically have lower requirements on availability and integrity.

The European Commission has recently launched a roadmap for the digitisation of the energy sector which sets out key actions. This includes a system-wide 'digitalisation of energy' action plan that could accelerate the implementation of digital solutions and energy system integration across multiple energy carriers, infrastructures and consumption sectors.

Considering these technology advances and commission plans, is important that energy firms define levels of service expected from their cloud providers, such as latency to ensure availability, and cyber security. Outsourcing of infrastructures and services requires appropriate third-party management and contractual due diligence to ensure cyber risks are appropriately managed.

"The need for modernisation of the energy sector is largely driven by the growing use of renewable resources, and more complex power requirements that drive technologies like microgrids and virtual power plants."

The way forward

The start of this year has already seen disruption in the oil industry. A cyber-attack has impacted the flow of fuel across a total of 17 terminals across Germany and Amsterdam, with many cargo vessels being diverted to other terminals in the region. It is not only the diversion costs and delay in business operation that has impacted the business, but the pending significant post cyber breach remediation costs to help prevent a similar incident.

The introduction of NIS has helped improve cyber resilience within the energy sector, although there is still work to be done. There is a need for a common threat and risk framework, and improved threat intelligence and knowledge sharing in order to help understand and address the cyber threats and risks concerning the energy sector. This framework should be updated regularly due to the ever-changing threat landscape. This would help provide a consistent approach to protect not only the energy infrastructure but also ensure the data protection rights of citizens.

An effective common cyber response framework and a rationalised view of the required capacity and capabilities of human resources to help ensure these cyber risks can be adequately mitigated will also help strengthen cyber resilience in the Energy sector.

If you require any further information, please contact Minesh Pandya at mineshpandya@hka.com.